



Configurer SVM-scoped NDMP

ONTAP 9

NetApp
February 13, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/ontap/ndmp/enable-svm-scoped-ndmp-cluster-task.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Configurer SVM-scoped NDMP	1
Activer NDMP à portée SVM sur le cluster ONTAP	1
Activer les utilisateurs de sauvegarde pour l'authentification ONTAP NDMP	2
Configurer les LIF ONTAP pour NDMP à portée SVM	3

Configurer SVM-scoped NDMP

Activer NDMP à portée SVM sur le cluster ONTAP

Si le DMA prend en charge l'extension Cluster Aware Backup (CAB), vous pouvez sauvegarder tous les volumes hébergés sur différents nœuds d'un cluster en activant SVM-scoped NDMP, en activant le service NDMP sur le cluster (admin SVM) et en configurant les LIF de données et de contrôle.

Avant de commencer

L'extension CAB doit être prise en charge par le DMA.

Description de la tâche

La désactivation du mode node-scoped NDMP permet d'activer le mode SVM-scoped NDMP sur le cluster.

Étapes

1. Activer le mode NDMP SVM-scoped :

```
cluster1::> system services ndmp node-scope-mode off
```

Le mode NDMP SVM-scoped est activé.

2. Activer le service NDMP sur le SVM d'admin:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

Le type d'authentification est défini sur challenge par défaut, l'authentification en texte brut est désactivée.



Pour des communications sécurisées, vous devez maintenir l'authentification en texte brut désactivée.

3. Vérifier que le service NDMP est activé :

```
cluster1::> vserver services ndmp show
```

Vserver	Enabled	Authentication type
cluster1	true	challenge
vsl	false	challenge

Activer les utilisateurs de sauvegarde pour l'authentification ONTAP NDMP

Pour authentifier SVM-scoped NDMP depuis l'application de backup, un utilisateur administratif doit disposer des privilèges suffisants et d'un mot de passe NDMP.

Description de la tâche

Vous devez générer un mot de passe NDMP pour les utilisateurs admin de sauvegarde. Vous pouvez activer les utilisateurs admin de sauvegarde au niveau du cluster ou de la SVM et, si nécessaire, vous pouvez créer un nouvel utilisateur. Par défaut, les utilisateurs disposant des rôles suivants peuvent s'authentifier pour la sauvegarde NDMP :

- Au niveau du cluster : admin ou backup
- SVM individuels : vsadmin ou vsadmin-backup

Si vous utilisez un utilisateur NIS ou LDAP, l'utilisateur doit exister sur le serveur respectif. Vous ne pouvez pas utiliser un utilisateur Active Directory.

Étapes

1. Afficher les utilisateurs et autorisations admin actuels :

```
security login show
```

Pour en savoir plus, `security login show` consultez le ["Référence de commande ONTAP"](#).

2. Si nécessaire, créez un nouvel utilisateur de sauvegarde NDMP avec la commande `security login create` et le rôle approprié pour les privilèges des SVM au niveau du cluster ou individuels.

Vous pouvez spécifier un nom d'utilisateur de sauvegarde locale ou un nom d'utilisateur NIS ou LDAP pour l'`-user-or-group-name` paramètre.

La commande suivante crée l'utilisateur de sauvegarde `backup_admin1` avec le `backup` rôle pour l'ensemble du cluster :

```
cluster1::> security login create -user-or-group-name backup_admin1
-application ssh -authmethod password -role backup
```

La commande suivante crée l'utilisateur de sauvegarde `vsbackup_admin1` avec le `vsadmin-backup` rôle d'un SVM individuel :

```
cluster1::> security login create -user-or-group-name vsbackup_admin1
-application ssh -authmethod password -role vsadmin-backup
```

Entrez un mot de passe pour le nouvel utilisateur et confirmez.

Pour en savoir plus, `security login create` consultez le ["Référence de commande ONTAP"](#).

3. Générer un mot de passe pour la SVM d'admin via la commande `vserver services ndmp generate password`.

Le mot de passe généré doit être utilisé pour authentifier la connexion NDMP par l'application de sauvegarde.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

Vserver: cluster1
User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

Configurer les LIF ONTAP pour NDMP à portée SVM

Vous devez identifier les LIF qui seront utilisées pour établir une connexion de données entre les données et les ressources sur bande, et pour contrôler la connexion entre la SVM d'administration et l'application de sauvegarde. Après avoir identifié les LIF, vous devez vérifier que les règles de service et de basculement sont définies.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "[Gérez le trafic pris en charge](#)".

ONTAP 9.10.1 ou version ultérieure

Étapes

1. Identifier le LIF intercluster hébergé sur les nœuds en utilisant `network interface show` la commande avec le `-service-policy` paramètre.

```
network interface show -service-policy default-intercluster
```

Pour en savoir plus, `network interface show` consultez le "[Référence de commande ONTAP](#)".

2. Identifier la LIF de management hébergée sur les nœuds en utilisant `network interface show` la commande avec le `-service-policy` paramètre.

```
network interface show -service-policy default-management
```

3. S'assurer que le LIF intercluster inclut le `backup-ndmp-control` service :

```
network interface service-policy show
```

Pour en savoir plus, `network interface service-policy show` consultez le "[Référence de commande ONTAP](#)".

4. S'assurer que la règle de basculement est correctement définie pour l'ensemble des LIFs :

- a. Vérifier que la policy de basculement pour la LIF de cluster-management est définie sur `broadcast-domain-wide`, Et la policy pour les LIFs intercluster et node-management est définie sur `local-only` à l'aide du `network interface show -failover` commande.

La commande suivante affiche la politique de basculement pour les LIFs cluster-management, intercluster et node-management :

```

cluster1::> network interface show -failover

      Logical          Home          Failover          Failover
Vserver  Interface      Node:Port    Policy      Group
-----
cluster  cluster1_clus1  cluster1-1:e0a  local-only  cluster
                                         Failover

Targets:
      .....
cluster1  cluster_mgmt  cluster1-1:e0m  broadcast-  Default
                                         domain-wide
                                         Failover

Targets:
      .....
IC1          cluster1-1:e0a  local-only  Default
                                         Failover

Targets:
IC2          cluster1-1:e0b  local-only  Default
                                         Failover

Targets:
      .....
cluster1-1  c1-1_mgmt1  cluster1-1:e0m  local-only  Default
                                         Failover

Targets:
      .....
cluster1-2  c1-2_mgmt1  cluster1-2:e0m  local-only  Default
                                         Failover

Targets:
      .....

```

- a. Si les stratégies de basculement ne sont pas définies de manière appropriée, modifiez la stratégie de basculement en utilisant la commande `network interface modify` avec `-failover-policy` paramètre.

```

cluster1::> network interface modify -vserver cluster1 -lif IC1
          -failover-policy local-only

```

Pour en savoir plus, `network interface modify` consultez le "[Référence de commande ONTAP](#)".

5. Spécifier les LIFs requises pour la connexion de données à l'aide de `vserver services ndmp modify` commande avec `preferred-interface-role` paramètre.

```
cluster1::> vserver services ndmp modify -vserver cluster1  
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. Vérifiez que le rôle d'interface préféré est défini pour le cluster à l'aide de `vserver services ndmp show` commande.

```
cluster1::> vserver services ndmp show -vserver cluster1  
  
Vserver: cluster1  
NDMP Version: 4  
.....  
.....  
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9.9 ou version antérieure

Étapes

1. Identifier les LIF intercluster, cluster-management et node-management en utilisant la `network interface show` commande avec `-role` paramètre.

La commande suivante affiche les LIFs intercluster :

```
cluster1::> network interface show -role intercluster  
  
Logical Status Network Current  
Current Is  
Vserver Interface Admin/Oper Address/Mask Node  
Port Home  
-----  
-----  
cluster1 IC1 up/up 192.0.2.65/24 cluster1-1  
e0a true  
cluster1 IC2 up/up 192.0.2.68/24 cluster1-2  
e0b true
```

La commande suivante affiche la LIF cluster-management :

```
cluster1::> network interface show -role cluster-mgmt

      Logical          Status      Network      Current
Current Is
Vserver      Interface      Admin/Oper Address/Mask      Node
Port        Home
-----  -----
-----  -----
cluster1      cluster_mgmt      up/up      192.0.2.60/24      cluster1-2
e0M        true
```

La commande suivante affiche les LIFs de node-management :

```
cluster1::> network interface show -role node-mgmt

      Logical          Status      Network      Current
Current Is
Vserver      Interface      Admin/Oper Address/Mask      Node
Port        Home
-----  -----
-----  -----
-----  -----
cluster1      cluster1-1_mgmt1      up/up      192.0.2.69/24      cluster1-1
e0M        true
                  cluster1-2_mgmt1      up/up      192.0.2.70/24      cluster1-2
e0M        true
```

Pour en savoir plus, `network interface show` consultez le ["Référence de commande ONTAP"](#).

2. Vérifier que la politique de pare-feu est activée pour NDMP sur les (node-mgmt `LIFs intercluster, cluster-management (`cluster-mgmt) et node-management) :
 - a. Vérifiez que la politique de pare-feu est activée pour NDMP à l'aide de `system services firewall policy show` commande.

La commande suivante affiche la politique de pare-feu pour la LIF cluster-management :

```
cluster1::> system services firewall policy show -policy cluster

Vserver      Policy      Service      Allowed
-----      -----
cluster      cluster      dns          0.0.0.0/0
                           http         0.0.0.0/0
                           https        0.0.0.0/0
                           ndmp         0.0.0.0/0
                           ndmps        0.0.0.0/0
                           ntp          0.0.0.0/0
                           rsh          0.0.0.0/0
                           snmp         0.0.0.0/0
                           ssh          0.0.0.0/0
                           telnet        0.0.0.0/0

10 entries were displayed.
```

La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver      Policy      Service      Allowed
-----      -----
cluster1     intercluster dns          -
                           http         -
                           https        -
                           ndmp         0.0.0.0/0, ::/0
                           ndmps        -
                           ntp          -
                           rsh          -
                           ssh          -
                           telnet        -
```

9 entries were displayed.

La commande suivante affiche la politique de pare-feu pour la LIF node-management :

```
cluster1::> system services firewall policy show -policy mgmt

Vserver      Policy      Service      Allowed
-----      -----
cluster1-1    mgmt        dns        0.0.0.0/0, ::/0
                           http       0.0.0.0/0, ::/0
                           https      0.0.0.0/0, ::/0
                           ndmp       0.0.0.0/0, ::/0
                           ndmps      0.0.0.0/0, ::/0
                           ntp        0.0.0.0/0, ::/0
                           rsh        -
                           snmp      0.0.0.0/0, ::/0
                           ssh        0.0.0.0/0, ::/0
                           telnet     -
10 entries were displayed.
```

- b. Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du `system services firewall policy modify` commande avec `-service` paramètre.

La commande suivante active la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. S'assurer que la règle de basculement est correctement définie pour l'ensemble des LIFs :

- a. Vérifier que la policy de basculement pour la LIF de cluster-management est définie sur `broadcast-domain-wide`, Et la policy pour les LIFs intercluster et node-management est définie sur `local-only` à l'aide du `network interface show -failover` commande.

La commande suivante affiche la politique de basculement pour les LIFs cluster-management, intercluster et node-management :

```

cluster1::> network interface show -failover

      Logical          Home          Failover
Failover
Vserver   Interface      Node:Port      Policy
Group
-----
-----
cluster   cluster1_clus1    cluster1-1:e0a    local-only
cluster
                                         Failover
Targets:
      .....  

cluster1  cluster_mgmt      cluster1-1:e0m    broadcast-domain-
wide Default
                                         Failover
Targets:
      .....  

      IC1           cluster1-1:e0a    local-only
Default
                                         Failover
Targets:
      IC2           cluster1-1:e0b    local-only
Default
                                         Failover
Targets:
      .....  

cluster1-1 cluster1-1_mgmt1  cluster1-1:e0m    local-only
Default
                                         Failover
Targets:
      .....  

      cluster1-2 cluster1-2_mgmt1  cluster1-2:e0m    local-only
Default
                                         Failover
Targets:
      .....  


```

- Si les stratégies de basculement ne sont pas définies de manière appropriée, modifiez la stratégie de basculement en utilisant la commande `network interface modify` avec `-failover -policy` paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1  
-failover-policy local-only
```

Pour en savoir plus, `network interface modify` consultez le "["Référence de commande ONTAP"](#)".

4. Spécifier les LIFs requises pour la connexion de données à l'aide de `vserver services ndmp modify` commande avec `preferred-interface-role` paramètre.

```
cluster1::> vserver services ndmp modify -vserver cluster1  
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Vérifiez que le rôle d'interface préféré est défini pour le cluster à l'aide de `vserver services ndmp show` commande.

```
cluster1::> vserver services ndmp show -vserver cluster1  
  
Vserver: cluster1  
NDMP Version: 4  
.....  
.....  
Preferred Interface Role: intercluster, cluster-mgmt,  
node-mgmt
```

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUSSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.